IN THE UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF TENNESSEE

WINSOUTH CREDIT UNION, Individually and on Behalf of All Similarly Situated,	)	**CASE NO.:**
Plaintiff,	)	
vs.	)	
MAPCO EXPRESS, INC., and DELEK US HOLDINGS, INC.,	)	
Defendants.	)	

COMPLAINT – CLASS ACTION

WinSouth Credit Union (hereinafter, "Plaintiff"), individually and on behalf of a class of all similarly situated financial institutions, asserts the following in its Complaint against MAPCO Express, Inc. (hereinafter, "MAPCO") and Delek US Holdings, Inc. (hereinafter, "Delek"):

Summary of Action

1. In both known and unknown data security breaches,[1] thousands of credit cards and debit cards were compromised due to MAPCO and Delek's acts and omissions. Plaintiff brings this class action on behalf of itself and all similarly situated financial institutions (collectively, "Financial Institutions") seeking redress and damages caused by MAPCO and Delek's misrepresentations, unfair and deceptive acts and practices, negligence, breach of contract, and improper retention of certain customer confidential information in connection with that data security breach. MAPCO and Delek's failure to adequately safeguard customer confidential information and related data and MAPCO and Delek's failure to maintain adequate encryption, intrusion detection and prevention procedures in their computer systems caused the losses hereinafter set forth.

2. As a result of MAPCO and Delek's wrongful actions, customer information was accessed from MAPCO and Delek's computer systems. As a result, class member Financial Institutions have incurred significant losses associated with credit and debit card reissuance, customer reimbursement for fraud losses, lost interest and transaction fees (including lost interchange fees), lost

[1] On May 6, 2013, MAPCO and Delek announced security breaches that resulted in the loss of customer credit card and debit card account information for thousands of customers.

customers, administrative expenses associated with monitoring and preventing fraud, and administrative expenses in dealing with investigation, customer confusion, fraud claims, and card reissuance.

3. Plaintiff seeks to recover damages caused by Defendants' negligent misrepresentations, unfair and/or deceptive acts or practices in accordance with applicable state laws, negligence, and breach of contract.

4. Plaintiff also seeks a finding and injunctive relief enjoining Defendants from improperly retaining customer data.

Jurisdiction and Venue

5. This Court has jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. §1332(d), in that (1) the Class (as defined below) has more than one hundred Class members, (2) the amount at issue exceeds five million dollars exclusive of interest and costs, and (3) minimal diversity exists as Plaintiff and Defendants are citizens of different states.

6. Venue in the United States District Court for the Middle District of Tennessee is appropriate, pursuant to 28 U.S.C. §1391(a), in that the Defendants reside in the Middle District of Tennessee and a substantial part of the events or omissions giving rise to the claim occurred in the Middle District of Tennessee.

Parties

A. Representative Plaintiff

7. WinSouth Credit Union is a retail credit union with its principal place of business located in Gadsden, Alabama.

8. WinSouth Credit Union issued Visa debit cards to its customers.

B. Defendants

9. Defendant MAPCO Express, Inc. is a Tennessee corporation owned and operated by Delek US Holdings, Inc., with its headquarters at 7102 Commerce Way, Brentwood, Tennessee 37027. MAPCO operates convenience store or "c-store" chains in Tennessee, Mississippi, and throughout the southeastern United States. MAPCO operates convenience stores in at least seven states under the MAPCO Express®, MAPCO Mart®, East Coast®, Discount Food Mart™, Fast Food and Fuel™, Delta Express®, and Favorite Markets® brand names. MAPCO is one of the largest company-operated convenience store chains in the United States, and one of the leading "c-store" operators of the southeast. More than half of the retail segment's store locations are in Tennessee. MAPCO owns the real estate of more than half of the stores it operates.

10. Defendant Delek US Holdings, Inc. is a Tennessee corporation and the parent company of MAPCO Express, Inc., with its headquarters at 7102 Commerce Way, Brentwood, Tennessee 37027.

Class Action Allegations

11. Plaintiff brings this action on its own behalf and on behalf of all other financial institutions similarly situated for the purpose of asserting claims alleged herein on a common basis, pursuant to 28 U.S.C. §1332(d). The proposed Class (the "Class") is defined as:

> Financial institutions that have suffered damages and/or harm as a result of data breaches set forth herein with respect to personal and financial information of customers who used debit or credit cards at Mapco retail stores.

12. The named representative Plaintiff is a member of the Class it seeks to represent.

13. This action is brought and may be properly maintained as a class action pursuant to 28 U.S.C. §1332(d). This action satisfies the procedural requirements set forth by Fed. R. Civ. P. 23.

14. The conduct of Defendants has caused injury to members of the proposed Class. The proposed Class is so numerous that joinder of all members is impracticable.

15. There are substantial questions of law and fact common to the Class. These questions include, but are not limited to, the following:

a. whether Defendants failed to provide adequate security and/or protection for their computer systems containing customers' financial and personal data;

b. whether Defendants negligently misrepresented that they did not retain customer financial information and negligently represented that they provided security as to their computer systems to prevent intrusions;

c. whether conduct (action or inaction) of Defendants resulted in the unauthorized breach of their computer systems containing customers' financial and personal data;

d. whether Defendants knew or should have known of the vulnerability of their computer systems to breach;

e. whether Defendants knew or should have known of the risks to financial institutions inherent in failing to protect such financial and personal information;

f. whether Defendants improperly retained customer personal and financial information despite representations that they would not keep such information;

g. whether Defendants disclosed (or directly or indirectly caused to be disclosed) private financial and personal information of customers;

h. whether Plaintiff and members of the proposed Class have been damaged by the conduct of the Defendants; and

i. whether Defendants breached their duties to exercise reasonable and due care in obtaining, using, retaining, and safeguarding the personal and financial information of bank customers.

16. The claims of the representative Plaintiff are typical of the proposed Class. The same events and conduct that give rise to Plaintiff's claims and legal theories also give rise to the claims and legal theories of the proposed Class. They are representative of the claims of financial institutions that are members of the proposed Class.

17. The representative Plaintiff will fairly and adequately represent the interests of the proposed Class. There are no disabling conflicts of interest between the representative Plaintiff and the proposed Class.

18. The named representative is part of the proposed Class, possessed the same interests, and suffered the same injuries as Class members, making its interests coextensive with those of the Class. The interests of the representative Plaintiff and members of the proposed Class are aligned so that the motive and inducement to protect and preserve these interests are the same for each.

19. Common questions of law and fact predominate over individualized questions. A class action is superior to other methods for the fair and efficient adjudication of this controversy.

20. Plaintiff is represented by experienced counsel who are qualified to handle this case. The lawsuit will be capably and vigorously pursued by the representative Plaintiff and its counsel.

Factual Background

21. MAPCO and Delek US Holdings, Inc. operate retail fuel and convenience stores in the United States. They offer fountain drinks, coffee, sandwiches, snack items, beverages, beef burgers, cheese steaks, chicken, and ice creams as well as fuel and related services. The company was incorporated in 2001 and is headquartered in Brentwood, Tennessee. MAPCO operates as a subsidiary of Delek US Holdings, Inc.

22. On May 6, 2013, MAPCO first publicly announced that it had been hit by a wide-reaching security breach that could leave thousands of customers exposed to fraud and identify theft from transactions that date back to March 2013. MAPCO's press release stated, in relevant part:

> Convenience store operator MAPCO Express, Inc. ("MAPCO") has experienced a security breach by third-party hackers that may have compromised the credit/debit card information of certain MAPCO customers. MAPCO operates convenience stores in Tennessee, northern and central Alabama, northern Georgia, Arkansas, Virginia, southern Kentucky and northern Mississippi under the MAPCO Express®, MAPCO Mart®, East Coast®, Discount Food Mart™, Fast Food and Fuel™, Delta Express®, and Favorite Markets® brand names.

As noted in the release, through its investigation, MAPCO has learned the following with respect to the intrusion:

- The incident involves credit/debit card payments for transactions at MAPCO locations between March 19-25, April 14-15 and April 20-21.

- MAPCO is notifying potentially affected customers because information may have been stolen that can be used to initiate fraudulent credit and debit card transactions.

- Upon discovering the issue, MAPCO took immediate steps to investigate the incident and further strengthened the security of its payment card processing systems to block future information security attacks.

- MAPCO is working with nationally recognized computer forensics investigation firms and the payment card associations to determine what happened and the extent of the information that may have been compromised.

- MAPCO is also working with law enforcement, including the FBI's Joint Cyber Crime Task Force, to identify the perpetrator.

23. MAPCO's press release also stated that after the security breach occurred, the Company "further strengthened the security of its payment card processing systems." The Company did not specify the nature of the improvements.

24. U.S. retailers, including MAPCO and Delek, are required to follow stringent card-industry rules. The rules that cover transactions on cards branded with logos from VISA, MasterCard International, Inc., American Express Co. and Discovery Financial Services, and others, require merchants to validate a series of security measures, such as the establishment of firewalls to protect databases. Among other things, merchants are prohibited from storing unprotected cardholder information.

25. Plaintiff has suffered unauthorized transactions and has incurred expenses and the loss of time related to changing cards and accounts because of Defendants' breach.

26. The security breach at MAPCO is currently being investigated by the Federal Bureau of Investigation and other law enforcement agencies.

27. Plaintiff's customers made purchases at MAPCO facilities during the relevant time period and did so because they were led to believe that the Defendants would not allow personal and private information to be disseminated to other unknown persons or entities.

28. MasterCard, Inc. ("MasterCard") is a publicly traded Delaware corporation that supports MasterCard credit and debit cards issued by financial institutions ("Issuing Banks") to consumers and processes transactions made with

those cards on behalf of financial institutions ("Acquiring Banks") that acquire the card-paid transactions of a merchant enrolled in MasterCard's program ("MasterCard Merchant"). VISA Inc. ("VISA") is a publicly traded Delaware corporation that supports VISA credit and debit cards issued by financial institutions ("Issuing Banks") to consumers and processes transactions made with those cards on behalf of financial institutions ("Acquiring Banks") that acquire the card-paid transactions of a merchant enrolled in VISA's program ("VISA Merchant").

29. Financial Institutions serve as Issuing Banks, which issue debit cards to their customers.

30. MAPCO and Delek, sellers of retail goods, are MasterCard and VISA Merchants and accept MasterCard and VISA card transactions from customers.

31. MasterCard issues regulations that are contained in "MasterCard International Bylaws and Rules," "MasterCard International Security Rules and Procedures," "MasterCard International Authorization System Manual," "MasterCard International Payment Card Industry Data Security Standard," and "MasterCard International Operating Regulations" ("MasterCard Operating Regulations"). Likewise, VISA issues regulations that are contained in "VISA International Operating Regulations" ("VISA Operating Regulations").

32. The MasterCard and VISA Operating Regulations governed the conduct of MAPCO and Delek at all times relevant to this action.

33. MAPCO and Delek are required to comply with the MasterCard and VISA Card Operating Regulations, including those portions of the Card Operating Regulations that mandate safeguarding of cardholder information and that prohibit retention or storage of unprotected cardholder information.

34. MasterCard states on its website, "A key focus of [MasterCard's security program] . . . is to ensure that Merchants and Service Providers are securely storing MasterCard account data in accordance with the Payment Card Industry Data Security Standard (PCI Data Security Standards)." *See* http://www.mastercard.com/us/sdp/index.html. Likewise, VISA International Operating Regulations require that all records that contain account or transaction information must be maintained in a safe and secure manner as specified in the PCI Standards. *See* http://usa.visa.com/merchants/merchant-support/international-operating-regulations.jsp.

35. The PCI Data Security Standards require the following:

Build and Maintain a Secure Network

- Install and maintain a firewall configuration to protect data

- Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

- Protect stored data
- Encrypt transmission of cardholder data and sensitive information across public networks

Maintain a Vulnerability Management Program

- Use and regularly update anti-virus software
- Develop and maintain secure systems and applications

Implement Strong Access Control Measures

- Restrict access to data by business need-to-know
- Assign a unique ID to each person with computer access
- Restrict physical access to cardholder data

Regularly Monitor and Test Networks

- Track and monitor all access to network resources and cardholder data
- Regularly test security systems and processes

Maintain an Information Security Policy

- Maintain a policy that addresses information security

36. At all times relevant hereto, MAPCO and Delek knew or should have known that the MasterCard and VISA Card Operating Regulations forbid them from retaining or storing MasterCard or VISA card magnetic stripe information subsequent to the authorization of a transaction.

37. At all times relevant hereto, MAPCO and Delek knew or should have known that the MasterCard and VISA Card Operating Regulations forbid them from disclosing any MasterCard or VISA cardholder account numbers, personal information, magnetic stripe information, or transaction information to third parties other than the merchant's agent, the Acquiring Bank, or the Acquiring Bank's agents.

38. At all times relevant hereto, MAPCO and Delek knew or should have known that the MasterCard or VISA Card Operating Regulations require them to secure and keep confidential cardholder information and magnetic stripe information from unauthorized disclosure, as set out in the Operating Regulations.

39. Defendants contract for participation in credit and debit card clearing systems and their involvement in this complex web of interrelated financial institutions required that Defendants: (a) comply with the Card Operating Regulations; (b) properly secure MasterCard and VISA card magnetic stripe

information; (c) not retain or store such information subsequent to authorization of a transaction; and (d) not disclose such information to unauthorized third parties.

40. MAPCO and Delek, at all times relevant to this action, represented and had a duty to Financial Institutions to: (a) comply with the Card Operating Regulations; (b) properly secure MasterCard and VISA card magnetic stripe information; (c) not retain or store such information subsequent to authorization of a transaction; and (d) not disclose such information to unauthorized third parties.

41. MAPCO and Delek negligently allowed MasterCard and VISA card magnetic stripe information to be compromised.

42. MAPCO and Delek negligently utilized a computer system that retained, stored, and/or disclosed (or allowed to be disclosed) MasterCard and VISA card magnetic stripe information.

43. The MasterCard and VISA cards from which MAPCO and Delek retained magnetic stripe information included thousands of cards issued by Issuing Banks to their customers. A substantial number of Issuing Banks' customers used the MasterCard and VISA cards at MAPCO stores and those transactions enabled MAPCO and Delek to retain and store information from those MasterCard cardholders through the magnetic stripe on the cards.

44. Data from the magnetic stripe on thousands of MasterCard and VISA cards, issued by Financial Institutions to their customers and used by those customers at MAPCO stores, was accessed from MAPCO and Delek.

45. Third parties were able to access, obtain, and use the MasterCard and VISA card magnetic stripe information obtained to fraudulently make transactions and to sell, transfer, use, or attempt to use such information for fraudulent purposes.

46. In accordance with its operating procedures, Issuing Banks receive notification of security breaches impacting MasterCard and VISA issued debit and credit cards through a system of alerts, known as Compromised Account Management System Alerts or "CAMS Alerts." CAMS Alerts: (a) identify generally the type of information compromised; (b) identify the timeframe such information was compromised; and (c) provide the Issuing Banks with a list of card numbers that it has issued that have been exposed to fraud risk.

47. In accordance with its operating procedures, MasterCard and VISA notifies Issuing Banks of security breaches impacting issued debit and credit cards through a security alert.

48. A substantial number of Financial Institutions' customers used the MasterCard and VISA cards at Defendants' stores and those transactions enabled

Defendants to retain and store information from those cardholders through the magnetic stripe on the MasterCard and VISA cards.

49. As a result of the events set forth in Paragraphs 1 through 50 of this Complaint, Financial Institutions and members of the proposed Class, to protect their customers and avoid fraud losses, cancelled MasterCard and VISA cards they had issued. Financial Institutions and members of the proposed Class reissued cards with new account numbers and magnetic stripe information to customers.

50. The cancellation and reissuance of cards resulted in damages and losses to Financial Institutions and members of the proposed Class of up to $30 per card.

51. As a result of the events set forth in Paragraphs 1 through 50 of this Complaint, Financial Institutions and members of the proposed Class suffered losses related to reimbursement of fraudulent charges or reversal of customer charges.

52. Financial Institutions and members of the proposed Class suffered losses related to lost interest and transaction fees (including lost interchange fees).

53. Financial Institutions and members of the proposed Class suffered losses related to administrative expenses and overhead charges associated with monitoring and preventing fraud.

54. Financial Institutions and members of the proposed Class suffered losses related to administrative expenses associated with addressing customer confusion and fraud claims.

55. Financial Institutions and members of the proposed Class have incurred additional costs, expenses, and other consequential damages, including, but not limited to, potential damages to Financial Institutions' reputations and lost customers.

56. Financial Institutions and members of the proposed Class will suffer additional monetary harm for the costs and expenses described above as additional fraud alerts and fraud charges are discovered and occur.

COUNT ONE
NEGLIGENT MISREPRESENTATION

57. Plaintiff incorporates Paragraphs 1 through 56 of this Complaint by reference herein.

58. In participating in the MasterCard and VISA Systems, MAPCO and Delek falsely represented that they would comply with the Card Operating Regulations and would safeguard customer data in order to induce Financial Institutions to act as Issuing Banks and provide their customers with MasterCard and VISA cards for use at MAPCO Stores. MAPCO made these representations in

the course of its business operations and had a pecuniary interest in the representations in that they would allow MAPCO to process payments from its customers.

59. MAPCO and Delek's compliance with the MasterCard and VISA Card Operating Regulations and safeguarding of customer data were material facts upon which the Financial Institutions (the Issuing Banks) relied. Further, MAPCO's representations that they would comply with the Card Operating Regulations and safeguard customer data were false at the time MAPCO made these representations to the Issuing Banks.

60. MAPCO and Delek, which knew or should have known that they were not in compliance with the Card Operating Regulations and were not safeguarding customer data, represented that they were so doing, which included a representation that it would not retain, store, or disclose the magnetic stripe information and would maintain the confidentiality of the information.

61. Financial Institutions agreed to act as the Issuing Banks for MasterCard and VISA card transactions expecting that large retail chains such as MAPCO and Delek would comply with the Card Operating Regulations and would safeguard customer data. Financial Institutions relied upon and acted in reliance on such representations by MAPCO and Delek.

62. Financial Institutions would have attempted to take additional steps to protect themselves but for the misrepresentations of MAPCO and Delek as set forth above.

63. MAPCO and Delek failed to exercise reasonable care in obtaining and in communicating the information that Financial Institutions relied upon.

64. Financial Institutions justifiably relied upon the false representations made by MAPCO and Delek regarding the security and confidentiality of the MasterCard and VISA card information.

65. Plaintiff and members of the proposed Class have suffered damages as set forth above as a result of MAPCO and Delek's misrepresentations.

COUNT TWO
VIOLATION OF THE GRAMM-LEACH-BLILEY ACT AS UNLAWFUL DECEPT ACTS AND PRACTICES

66. Plaintiff incorporates Paragraphs 1 through 65 of this Complaint by reference herein.

67. Defendants have a duty pursuant to the Gramm-Leach-Bliley Act, 15 U.S.C. §6801 *et seq*. and 16 C.F.R. §313 *et seq*., not to misuse or inappropriately

disclose information received as a third party for the purpose of processing a transaction requested by a customer of its stores.

68. Pursuant to 16 C.F.R. §313.11(iii), third-party recipients of financial data, such as Defendants, cannot "use" or "disclose" the information other than in "the ordinary course of business to carry out the activity covered by the exception under which [it] received the information."

69. Defendants were obligated under 16 C.F.R. §313.11 to ***only*** use and disclose customer financial information for the purposes for which it was disclosed, more specifically, to process the transaction.

70. Financial Institutions, in the course of business, placed the nonpublic personal information of their cardholder-customers onto the magnetic stripe of their cards with the expectation that retail merchants, such as Defendants, would access that information only for the purpose of processing transactions that are initiated by that customer.

71. Defendants violated the Gramm-Leach-Bliley Act in that they improperly used and disclosed the information in violation of the Privacy Regulations by (i) maintaining the data well beyond the permitted timeframe; and (ii) allowing the data to be accessed by others for purposes unrelated to the processing of the credit or debit transaction.

72. Plaintiff and members of the proposed Class have suffered damages as set forth above as a result of these unfair and deceptive trade practices.

73. The unfair and deceptive acts and practices described above were knowingly unfair and/or willful.

COUNT THREE
NEGLIGENCE

74. Plaintiff incorporates Paragraphs 1 through 74 of this Complaint by reference herein.

75. Defendants owed a duty to Financial Institutions to use and exercise reasonable and due care in obtaining and retaining the personal and financial information of Financial Institutions and their customers.

76. Defendants owed a duty to Financial Institutions to provide adequate security to protect the personal and financial information of Financial Institutions and their customers.

77. Defendants breached their duties by allowing an unlawful intrusion into their computer system, failing to protect against such an intrusion; and

allowing personal and financial information of Financial Institutions and their customers to be accessed by third parties.

78. Defendants knew, or with the reasonable exercise of care should have known, of the risks inherent in retaining such information, and the importance of providing adequate security.

79. As a direct and proximate result of Defendants' carelessness and negligent conduct, Plaintiff and members of the proposed Class suffered substantial losses as set forth above.

COUNT FOUR
NEGLIGENCE PER SE

80. Plaintiff incorporates Paragraphs 1 through 79 of this Complaint by reference herein.

81. At all relevant times, Defendants were required to comply with, inter alia, the applicable industry standards requiring Defendants to implement internal system controls to prevent, detect, and responds to system intrusions, and to securely handle and transfer sensitive financial data of their customers. These standards include, without limitation, the PCI Standards and the Card Operating Regulations.

82. Defendants were also required to comply with federal regulations governing the protection of consumer information, including, without limitation, the 16 C.F.R. §681, more commonly referred to as the "Red Flag Rules." The Red Flag Rules require Defendants to adopt a plan to prevent identity theft and ensure the safety of its customer's financial and personal data. The Red Flag Rules require "creditors" and "financial institutions" with "covered accounts" to implement programs to identify, detect, and respond to the warning signs or "red flags" that could indicate potential identity theft. At all relevant times, Defendants were "creditors" and had "covered accounts" as used in the Red Flag Rules. Under the relevant Red Flag Rules, Defendants were required to "oversee, develop, and administer" a written Identity Theft Protection Program that identifies and addresses "red flags" indicating vulnerabilities and potential security threats to, among other information, sensitive financial information of Defendants' customers. Further, the Red Flag Rules require that the Defendants' written Identity Theft Protection Program include provisions for detecting red flags, including procedures for monitoring credit transactions, as well as responding to and mitigating the instances of potential identity theft.

83. The regulations and industry security standards set forth in Paragraphs 81 and 82 establish the minimal duty of care owed by Defendants to Plaintiff and members of the Class.

84. Defendants failed to comply with the stated regulations and industry security standards as more fully described above.

85. Upon information and belief, had Defendants been in compliance with the regulations and industry security standards during the relevant time period, the Data Breach would not have occurred.

86. Defendants' violations of the PCI Standards, the Card Operating Regulations, and the Red Flag Rules constitute negligence per se and directly and/or proximately caused Plaintiff and members of the Class to suffer substantial damages.

87. Plaintiff and members of the Class were members of the class of persons intended to be protected by the PCI Standards, the Card Operating Regulations, and the Red Flag Rules.

88. As a direct and proximate result of Defendants' carelessness and negligent conduct, Plaintiff and members of the proposed Class suffered substantial losses as set forth above.

COUNT FIVE
BREACH OF CONTRACT

89. Plaintiff incorporates Paragraphs 1 through 88 of this Complaint by reference herein.

90. Defendants were required to comply with the MasterCard and VISA Card Operating Regulations.

91. Defendants breached their obligations to Financial Institutions as third-party beneficiaries of Defendants' contract with card clearing entities.

92. Plaintiff and the Class were intended third-party beneficiaries to the contracts entered into by MAPCO to comply with the Card Operating Regulations and such contracts are valid and enforceable.

93. As a direct and proximate result of Defendants' breach of contract, Plaintiff and members of the proposed Class suffered losses as set forth above.

PRAYER FOR RELIEF

WHEREFORE, Financial Institutions and members of the proposed Class seek damages against the Defendants for the conduct detailed herein. Plaintiff demands judgment against Defendants as follows:

A. Certification of the Class under Fed. R. Civ. P. 23 and appointment of Plaintiff as representatives of the Class and its counsel as lead Class counsel pursuant to Fed. R. Civ. P. 23(g);

B. Money damages;

C. Reasonable attorney's fees;

D. Costs;

E. Prejudgment interest; and

F. Such other relief as the Court deems equitable and just.

JURY DEMAND

Pursuant to Fed. R. Civ. P. 38(b) Plaintiff demands a trial by jury on all issues so triable.

J. Gerard Stranch, IV (BPR #023045)
Benjamin A. Gastel (BPR# 028699)
Branstetter, Stranch & Jennings, PPLC
227 Second Avenue North, 4th Floor
Nashville, TN 37201-1631
Telephone: 615-254-8801
Facsimile: 615-250-3937
gerards@branstetterlaw.com
beng@branstetterlaw.com

Joseph P. Guglielmo
Scott+Scott, Attorneys At Law, LLP
The Chrysler Building
405 Lexington Avenue, 40th Floor
New York, NY 10174
Telephone: 212-223-6444
Facsimile: 212-223-6334
jguglielmo@scott-scott.com

Attorneys for Plaintiff